

Private-Capacity Bounds for Bosonic Wiretap Channels

Ligong Wang, *Member IEEE*, Jeffrey H. Shapiro, *Life Fellow IEEE*,

Nivedita Chandrasekaran, Gregory W. Wornell, *Fellow IEEE*

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA

{wlg, jhs, nivedita, gww}@mit.edu

Abstract—We prove an upper bound on the private capacity of the single-mode noiseless bosonic wiretap channel. Combined with a previous lower bound, we obtain the low photon-number asymptotic expression for the private capacity. We then show that the multiple-mode noiseless bosonic wiretap channel is equivalent to parallel single-mode channels, hence the single-mode bounds can be applied. Finally, we consider multiple-spatial-mode propagation through atmospheric turbulence, and derive a private-capacity lower bound that only requires second moments of the channel matrix.

I. INTRODUCTION

In a variety of emerging applications, there is a need for secure transmission over optical links. In such settings, a natural approach to providing security against computationally-unbounded attacks is to exploit the physical layer, and the corresponding natural information theoretic model for analysis is the basic bosonic wiretap channel. In practice, a variety of regimes are of interest. While for optical links photon efficiency (b/photon) has tended to be of greater importance than spectral efficiency (b/s/Hz), there is growing interest in the latter as well. When the photon and spectral efficiency requirements are simultaneously high, multiple spatial modes are required [1]. Accordingly there is a need to more fully understand the capacity of both single-mode and multiple-mode bosonic wiretap channels in such regimes. Moreover, in practice, free-space propagation is strongly affected by turbulence, the effect of which on private capacity is also not yet well understood.

In this paper, we first prove an upper bound on the private capacity of the single-mode bosonic wiretap channel. Combining our upper bound with the previously-derived lower bound [2], we obtain the single-mode private capacity's low photon-number asymptotic behavior. We then treat the multiple-mode bosonic wiretap channel, obtaining results that tightly bracket the private capacity when both high photon efficiency and high spectral efficiency are required. Finally, we exploit convexity and majorization to obtain a lower bound on the multiple-spatial-mode private capacity for the turbulent channel that only requires second moments of the channel matrix, and thus may be tight for near-field operation in which both high photon efficiency and high spectral efficiency are obtained.

II. NOTATION

We use a lower-case letter like x to denote a number, and an upper-case letter like X to denote a random variable (except

for some special cases, e.g., C denotes the capacity). We use a boldface lower-case letter like \mathbf{x} or $\boldsymbol{\eta}$ to denote a vector, and a boldface upper-case letter like \mathbf{X} or \mathbf{H} to denote a random vector. We use a font like \mathbf{t} to denote a matrix, and a corresponding upper-case letter like \mathbf{T} to denote a random matrix. Finally, we use a font like \mathbb{A} to denote a Hilbert space, a font like \hat{a} to denote the annihilation operator on \mathbb{A} , and $\hat{\rho}^{\mathbb{A}}$ to denote a density operator on \mathbb{A} .

All logarithms in this paper are natural logarithms, and information is measured in nats unless stated otherwise.

III. THE SINGLE-MODE CHANNEL

A. Channel Model and Previous Work

Let \hat{a} , \hat{b} , and \hat{e} denote the annihilation operators on the Hilbert spaces of Alice, Bob, and Eve, respectively. The single-mode noiseless bosonic wiretap channel can be described in the Heisenberg picture by the beam splitter relation

$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{v}, \quad (1a)$$

$$\hat{e} = \sqrt{1-\eta}\hat{a} - \sqrt{\eta}\hat{v}, \quad (1b)$$

where $\eta \in [0, 1]$, and where \hat{v} is the annihilation operator of the noise mode, which we assume to be in its vacuum state. Note that this is a *worst-case* model in the sense that we assume Eve can obtain all photons that do not reach Bob. We impose an average-photon-number constraint on the input

$$\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{n}, \quad (2)$$

where the expectation is averaged over all codewords. Denote the classical private capacity of the channel (1) under constraint (2) by $C_P(\eta, \bar{n})$. It is shown in [2] that

$$C_P(\eta, \bar{n}) \geq L(\eta, \bar{n}), \quad (3)$$

with

$$L(\eta, \bar{n}) = \begin{cases} g(\eta\bar{n}) - g((1-\eta)\bar{n}), & \eta > 1/2, \\ 0, & \text{otherwise,} \end{cases} \quad (4)$$

where

$$g(x) \triangleq (1+x) \log(1+x) - x \log x, \quad x > 0 \quad (5)$$

is the maximum entropy of a single-mode bosonic state whose expected photon-number equals x , achieved by the *thermal state*:

$$\hat{\rho} = \sum_{n=0}^{\infty} \frac{x^n}{(x+1)^{n+1}} |n\rangle\langle n|, \quad (6)$$

where $|n\rangle$ denotes the number state containing n photons.

It is conjectured in [2] that (3) holds with equality, as a consequence of the conjectured “Entropy Photon-Number Inequality”.

As \bar{n} tends to infinity, the lower bound (3) is tight and agrees with the private-capacity formula derived in [3]:

$$C_P(\eta, \infty) = \max \{0, \log(\eta) - \log(1 - \eta)\}. \quad (7)$$

B. An Upper Bound on $C_P(\eta, \bar{n})$

Theorem 1: The classical private capacity $C_P(\eta, \bar{n})$ is bounded by

$$C_P(\eta, \bar{n}) \leq U(\eta, \bar{n}), \quad (8)$$

where

$$U(\eta, \bar{n}) \triangleq \begin{cases} g((2\eta - 1)\bar{n}), & \eta > 1/2, \\ 0, & \text{otherwise.} \end{cases} \quad (9)$$

Before proving Theorem 1, we first prove a simple lemma which says that $C_P(\eta, \bar{n})$ is monotonic in η .

Lemma 1: For any $1 \geq \eta_1 \geq \eta_2 \geq 0$ and any $\bar{n} > 0$,

$$C_P(\eta_1, \bar{n}) \geq C_P(\eta_2, \bar{n}). \quad (10)$$

Proof: Let \mathbb{B}_i and \mathbb{E}_i denote the output Hilbert spaces of Bob and Eve, respectively, of the channel with transmissivity (from Alice to Bob) η_i , $i = 1, 2$. Observe that \mathbb{B}_2 is stochastically degraded from \mathbb{B}_1 . Indeed, when we pass the state on \mathbb{B}_1 through a beam splitter of transmissivity η_2/η_1 , we obtain a state that is identical to the one on \mathbb{B}_2 . Therefore, a Bob having access to \mathbb{B}_1 can always pass his state through this beam splitter and then make the same measurement as a Bob having access to \mathbb{B}_2 , thus he can do *at least* as well as the latter. Similarly, \mathbb{E}_1 is stochastically degraded from \mathbb{E}_2 , and an Eve having access to \mathbb{E}_1 can do *at most* as well as an Eve having access to \mathbb{E}_2 . Hence we obtain (10). ■

Proof of Theorem 1: By Lemma 1, we only need to prove the case where $\eta > 1/2$. In this case the wiretap channel is stochastically degraded. To see this, we pass Bob’s state through another beam splitter to obtain output modes with annihilation operators \hat{e}' and \hat{c} given by

$$\hat{e}' = \sqrt{\eta'}\hat{b} + \sqrt{1 - \eta'}\hat{v}', \quad (11a)$$

$$\hat{c} = \sqrt{1 - \eta'}\hat{b} - \sqrt{\eta'}\hat{v}', \quad (11b)$$

where $\eta' \triangleq (1 - \eta)/\eta \in [0, 1)$ as we assume $\eta > 1/2$, and \hat{v}' is in its vacuum state. Then the states $\hat{\rho}^{\mathbb{B}}$ and $\hat{\rho}^{\mathbb{E}'}$ are identical for any input state $\hat{\rho}^{\mathbb{A}}$. See Fig. 1.

We now prove (8) as follows:

$$C_P(\eta, \bar{n}) = \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{n}} [S(\hat{\rho}^{\mathbb{B}}) - S(\hat{\rho}^{\mathbb{E}})] \quad (12)$$

$$= \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{n}} [S(\hat{\rho}^{\mathbb{B}}) - S(\hat{\rho}^{\mathbb{E}'})] \quad (13)$$

$$= \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{n}} [S(\hat{\rho}^{\mathbb{B}} \otimes |0\rangle\langle 0|^{\mathbb{V}'}) - S(\hat{\rho}^{\mathbb{E}'})] \quad (14)$$

$$= \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{n}} [S(\hat{\rho}^{\mathbb{E}'\mathbb{C}}) - S(\hat{\rho}^{\mathbb{E}'})] \quad (15)$$

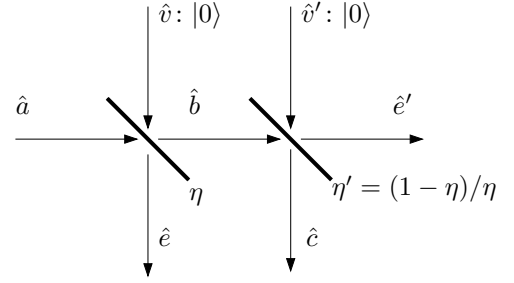


Fig. 1. Illustration of the degraded wiretap channel.

$$\leq \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{n}} [S(\hat{\rho}^{\mathbb{E}'}) + S(\hat{\rho}^{\mathbb{C}}) - S(\hat{\rho}^{\mathbb{E}'})] \quad (16)$$

$$= \max_{\langle \hat{a}^\dagger \hat{a} \rangle \leq \bar{n}} S(\hat{\rho}^{\mathbb{C}}) \quad (17)$$

$$= g((2\eta - 1)\bar{n}), \quad (18)$$

where $S(\hat{\rho}) = -\text{Tr}[\hat{\rho} \log(\hat{\rho})]$ is the von Neumann entropy. The steps are justified as follows: (12) follows from [4, Theorem 2]; (13) from the fact that $\hat{\rho}^{\mathbb{B}}$ and $\hat{\rho}^{\mathbb{E}'}$ are identical; (14) because $|0\rangle\langle 0|^{\mathbb{V}'}$ is a pure state; (15) because the beam splitter (11) is a unitary transformation from $\hat{\rho}^{\mathbb{B}\mathbb{V}'}$ to $\hat{\rho}^{\mathbb{E}'\mathbb{C}}$; (16) from the subadditivity of von Neumann entropy; and (18) because, according to the channel laws (1) and (11),

$$\hat{c} = \sqrt{2\eta - 1}\hat{a} + \sqrt{\frac{(2\eta - 1)(1 - \eta)}{\eta}}\hat{v} - \sqrt{\frac{1 - \eta}{\eta}}\hat{v}', \quad (19)$$

so

$$\langle \hat{c}^\dagger \hat{c} \rangle = (2\eta - 1)\langle \hat{a}^\dagger \hat{a} \rangle \leq (2\eta - 1)\bar{n}. \quad (20)$$

■

C. Analysis of the Bounds

Combining the upper and lower bounds (8) and (3) and letting \bar{n} tend to zero, we obtain the asymptotic expression for $C_P(\eta, \bar{n})$ when \bar{n} is small.

Theorem 2: The private capacity $C_P(\eta, \bar{n})$ satisfies

$$C_P(\eta, \bar{n}) = (2\eta - 1)\bar{n} \log \frac{1}{\bar{n}} + O(\bar{n}), \quad (21)$$

where $O(\bar{n})$ is a function of η and \bar{n} satisfying

$$\begin{aligned} \eta \left(1 + \log \frac{1}{\eta} \right) - (1 - \eta) \left(1 + \log \frac{1}{1 - \eta} \right) &\leq \lim_{\bar{n} \downarrow 0} \frac{O(\bar{n})}{\bar{n}} \\ &\leq \lim_{\bar{n} \downarrow 0} \frac{O(\bar{n})}{\bar{n}} \leq (2\eta - 1) \left(1 + \log \frac{1}{2\eta - 1} \right). \end{aligned} \quad (22)$$

Theorem 2 shows that the *photon efficiency*, $C_P(\eta, \bar{n})/\bar{n}$, behaves like $\log(1/\bar{n})$ plus some constant for small \bar{n} . We numerically compare the upper and lower bounds (8) and (3) on the photon efficiency against \bar{n} for $\eta = 0.7$ in Fig. 2, and against η for $\bar{n} = 10^{-3}$ in Fig. 3.

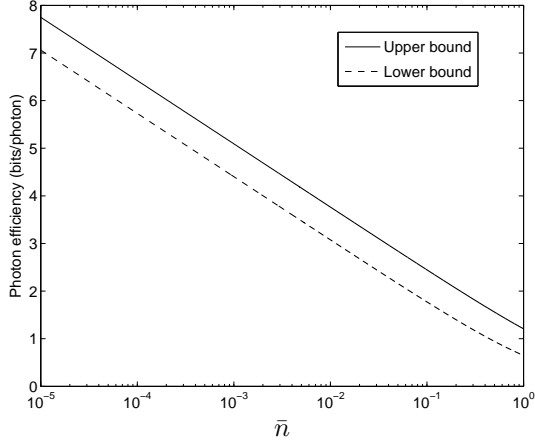


Fig. 2. Comparison of the upper and lower bounds on the photon efficiency (in bits per photon) computed from (8) and (3) for $\eta = 0.7$.

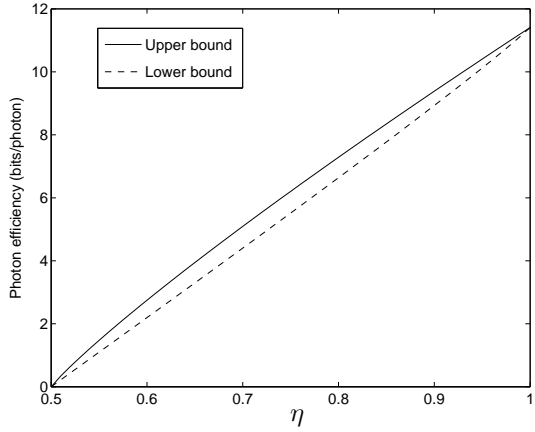


Fig. 3. Comparison of the upper and lower bounds on the photon efficiency (in bits per photon) computed from (8) and (3), for $\bar{n} = 10^{-3}$.

IV. THE MULTIPLE-MODE CHANNEL

A. Channel Model

Consider a multiple-mode noiseless bosonic wiretap channel in which Alice's, Bob's, and Eve's modes are described by annihilation operators $\{\hat{a}_1, \dots, \hat{a}_m\}$, $\{\hat{b}_1, \dots, \hat{b}_k\}$, and $\{\hat{e}_1, \dots, \hat{e}_l\}$, respectively. The channel law is a multiple-mode beam splitter relation, i.e.,

$$\begin{pmatrix} \hat{b}_1 \\ \vdots \\ \hat{b}_k \\ \hat{e}_1 \\ \vdots \\ \hat{e}_l \end{pmatrix} = \begin{pmatrix} t_{ab} & t_{vb} \\ t_{ae} & t_{ve} \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \vdots \\ \hat{a}_m \\ \hat{v}_1 \\ \vdots \\ \hat{v}_{k+l-m} \end{pmatrix}, \quad (23)$$

where

$$t \triangleq \begin{pmatrix} t_{ab} & t_{vb} \\ t_{ae} & t_{ve} \end{pmatrix} \quad (24)$$

is a unitary matrix, and where $\{\hat{v}_1, \dots, \hat{v}_{k+l-m}\}$ are annihilation operators of vacuum-state noise modes. Note that this

is again a worst-case model in which Eve obtains all photons that do not reach Bob.

B. Simplification of Channel Model

The next theorem shows that any multiple-mode noiseless bosonic wiretap channel is equivalent to a group of parallel (i.e., noninterfering) single-mode channels.

Theorem 3: The channel (23) is equivalent to a group of parallel single-mode channels:

$$\hat{b}'_i = \sqrt{\eta_i} \hat{a}'_i + \sqrt{1 - \eta_i} \hat{v}'_i, \quad (25a)$$

$$\hat{e}'_i = \sqrt{1 - \eta_i} \hat{a}'_i - \sqrt{\eta_i} \hat{v}'_i, \quad (25b)$$

where $i \in \{1, \dots, m\}$, and where $\{\eta_1, \dots, \eta_m\}$ are the eigenvalues of $t_{ba}^\dagger t_{ba}$.

Proof: From the unitarity of the transition matrix t we have

$$\begin{pmatrix} t_{ab}^\dagger & t_{ae}^\dagger \\ t_{vb}^\dagger & t_{ve}^\dagger \end{pmatrix} \cdot \begin{pmatrix} t_{ab} & t_{vb} \\ t_{ae} & t_{ve} \end{pmatrix} = 1^{(k+l) \times (k+l)}, \quad (26)$$

so

$$t_{ab}^\dagger t_{ab} + t_{ae}^\dagger t_{ae} = 1^{m \times m}. \quad (27)$$

This implies that $t_{ab}^\dagger t_{ab}$ and $t_{ae}^\dagger t_{ae}$ are simultaneously diagonalizable. More specifically, there exists a unitary matrix v such that

$$v^\dagger t_{ab}^\dagger t_{ab} v = d, \quad (28)$$

$$v^\dagger t_{ae}^\dagger t_{ae} v = 1^{m \times m} - d, \quad (29)$$

where d is an $m \times m$ diagonal matrix whose diagonal terms are, by assumption, η_1, \dots, η_m . Therefore the matrices t_{ab} and t_{ae} have the same right singular vectors, and their singular-value decompositions can be written as

$$t_{ab} = u_{ab} s_{ab} v^\dagger, \quad (30)$$

$$t_{ae} = u_{ae} s_{ae} v^\dagger, \quad (31)$$

where u_{ab} and u_{ae} are unitary matrices, s_{ab} is a $k \times m$ diagonal matrix whose (nonzero) diagonal entries are (the nonzero elements of) $\{\sqrt{\eta_1}, \dots, \sqrt{\eta_m}\}$, and s_{ae} is an $l \times m$ diagonal matrix whose (nonzero) diagonal entries are (the nonzero elements of) $\{\sqrt{1 - \eta_1}, \dots, \sqrt{1 - \eta_m}\}$.

Now we observe that v^\dagger does not affect the private capacity of this channel. This is because Alice can perform v on the input light modes that she prepared to cancel v^\dagger simultaneously for Bob and Eve. Hence we can always set v^\dagger to be $1^{m \times m}$ without affecting the private capacity. Similarly, u_{ab} and u_{ae} can be canceled by Bob and Eve, respectively, so they can also be set to identity matrices without changing the private capacity. We thus conclude that the private capacity of (23) is the same as that of the parallel-mode channel (25). ■

C. Capacity Results

Denote the private capacity of the channel (23) under the average-photon-number constraint

$$\sum_{i=1}^m \langle \hat{a}_i^\dagger \hat{a}_i \rangle \leq \bar{n} \quad (32)$$

by $C_P^M(\mathbf{t}, \bar{n})$. By Theorem 3, it equals the capacity of the channel (25) under constraint

$$\sum_{i=1}^m \langle \hat{a}_i^\dagger \hat{a}_i \rangle \leq \bar{n}, \quad (33)$$

which we denote by $C_P^M(\boldsymbol{\eta}, \bar{n})$ where $\boldsymbol{\eta} \triangleq (\eta_1, \dots, \eta_m)^T$. We first show that $C_P^M(\boldsymbol{\eta}, \bar{n})$ is achievable by coding independently for each mode in (25).

Theorem 4: Coding independently for each mode in (25) is optimal:

$$C_P^M(\boldsymbol{\eta}, \bar{n}) = \max_{\substack{\bar{n}_i \geq 0, \\ \sum_{i=1}^m \bar{n}_i = \bar{n}}} \sum_{i=1}^m C_P(\eta_i, \bar{n}_i). \quad (34)$$

Proof: Let $\boldsymbol{\eta}'$ be

$$\eta'_i = \begin{cases} \eta_i, & \eta_i > 1/2, \\ 1/2, & \eta_i \leq 1/2. \end{cases} \quad (35)$$

By extending Lemma 1 to the multiple-mode scenario, we have

$$C_P^M(\boldsymbol{\eta}, \bar{n}) \leq C_P^M(\boldsymbol{\eta}', \bar{n}). \quad (36)$$

Next denote by $C_P^M(\boldsymbol{\eta}', \bar{n})$, where $\bar{\mathbf{n}} \triangleq (\bar{n}_1, \dots, \bar{n}_m)^T$, the capacity of the parallel-mode channel with transmissivities $\boldsymbol{\eta}'$ and *individual* photon-number constraints

$$\langle \hat{a}_i^\dagger \hat{a}_i \rangle \leq \bar{n}_i, \quad i = 1, \dots, m, \quad (37)$$

then

$$C_P^M(\boldsymbol{\eta}', \bar{n}) = \max_{\substack{\bar{n}_i \geq 0, \\ \sum_{i=1}^m \bar{n}_i = \bar{n}}} \sum_{i=1}^m C_P(\eta'_i, \bar{n}_i). \quad (38)$$

To simplify $C_P^M(\boldsymbol{\eta}', \bar{n})$, note that each individual channel of this parallel-mode channel is stochastically degraded, so the private capacities of the individual channels are *additive* [4]:

$$C_P^M(\boldsymbol{\eta}', \bar{n}) = \sum_{i=1}^m C_P(\eta'_i, \bar{n}_i). \quad (39)$$

We thus have

$$C_P^M(\boldsymbol{\eta}, \bar{n}) \leq \max_{\substack{\bar{n}_i \geq 0, \\ \sum_{i=1}^m \bar{n}_i = \bar{n}}} \sum_{i: \eta_i > 1/2} C_P(\eta'_i, \bar{n}_i) \quad (40)$$

$$= \max_{\substack{\bar{n}_i \geq 0, \\ \sum_{i=1}^m \bar{n}_i = \bar{n}}} \sum_{i: \eta_i > 1/2} C_P(\eta_i, \bar{n}_i), \quad (41)$$

where the equality follows because the optimal photon-number allocation is the same for the right-hand sides of both (40) and (41), which assigns zero photon to the modes where $\eta_i \leq 1/2$ (i.e., where $\eta'_i = 1/2$).

On the other hand, by coding independently, and using the optimal code for each mode, we can achieve the lower bound

$$C_P^M(\boldsymbol{\eta}, \bar{n}) \geq \max_{\substack{\bar{n}_i \geq 0, \\ \sum_{i=1}^m \bar{n}_i = \bar{n}}} \sum_{i: \eta_i > 1/2} C_P(\eta_i, \bar{n}_i). \quad (42)$$

Combining (41) and (42) proves (34). ■

Now it is straightforward to extend the upper and lower bounds (8) and (3) to the multiple-mode case. In particular,

in the limit as \bar{n} approaches zero, it is easy to check that the optimal photon-number allocation is the same for both the upper and the lower bounds, and it sends all photons in the mode with the largest transmissivity. We hence have the following asymptotic capacity expression.

Theorem 5: The capacity of the channel (23) under constraint (32) satisfies

$$C_P^M(\mathbf{t}, \bar{n}) = (2\eta_{\max} - 1)\bar{n} \log \frac{1}{\bar{n}} + O(\bar{n}), \quad (43)$$

where η_{\max} is the largest eigenvalue of $\mathbf{t}_{ab}^\dagger \mathbf{t}_{ab}$, and where the term $O(\bar{n})$ is at most linear in \bar{n} :

$$\lim_{\bar{n} \downarrow 0} \left| \frac{O(\bar{n})}{\bar{n}} \right| < \infty. \quad (44)$$

As an example of our multiple-mode private capacity bounds, consider the use of $m = 10^3$ high-transmissivity spatial modes with near-equal, near-unity eigenvalues, $(\eta_1, \dots, \eta_m)^T$, as exist for L m vacuum-propagation at wavelength λ between coaxial diameter- D circular pupils satisfying $(\pi D^2/4\lambda L)^2 \gg m$ [5]. Figure 4 shows that our results provide tight bounds on the photon efficiency and spectral efficiency for this example.

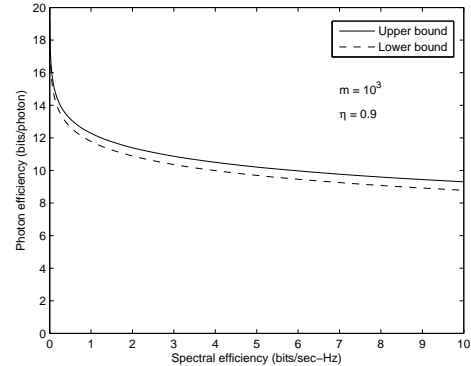


Fig. 4. Comparison of the upper and lower bounds for photon efficiency versus spectral efficiency for $m = 10^3$ spatial modes each with $\eta = 0.9$.

V. CHANNELS WITH TURBULENCE

A. Channel Model

Consider a multiple-mode wiretap channel in which the transition matrix \mathbf{t} in (24) is replaced by a random matrix \mathbf{T} . We assume a *coherent* scenario where Alice and Bob know the realization of \mathbf{T}_{ab} . Then, as discussed in Section IV-B, they also know the other parts of \mathbf{T} , namely, \mathbf{T}_{ae} , \mathbf{T}_{vb} and \mathbf{T}_{ve} except for possible unitary transformations that are irrelevant to capacity calculations. We impose the constraint that the average number of transmitted photons in *every* channel use must not exceed \bar{n} , irrespective of the realization of \mathbf{T}_{ab} . Denote by $\{H_1, \dots, H_m\}$ the random eigenvalues of $\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}$,

then the capacity of this channel can be expressed as

$$C_P^M(\mathbf{T}, \bar{n}) = \mathbb{E} \left[\max_{\substack{\bar{N}_i \geq 0, \\ \sum_{i=1}^m \bar{N}_i = \bar{n}}} C_P(H_i, \bar{N}_i) \right]. \quad (45)$$

For near-field operation—wherein the turbulent channel will support multiple spatial modes with appreciable eigenvalues [6]—the exact distribution of \mathbf{T}_{ab} is unavailable. Instead, we can only compute the second-moment matrix $\mathbb{E}[\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}]$. Our goal in this section is to find good bounds on the private capacity of the multiple-mode wiretap channel with turbulence expressed using $\mathbb{E}[\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}]$.

B. Lower Bound on Private Capacity

To derive a lower bound on the private capacity of this channel, we need two lemmas.

Lemma 2: The single-mode lower bound $L(\eta, \bar{n})$ as defined in (4) is convex in η for $\eta \in [0, 1]$ and for every $\bar{n} > 0$.

Proof: Since $L(\eta, \bar{n})$ is the constant zero and is hence convex in η for $\eta \in [0, \frac{1}{2}]$, we only need to check convexity for $\eta \in (\frac{1}{2}, 1]$. In the latter region,

$$L(\eta, \bar{n}) = g(\eta\bar{n}) - g((1-\eta)\bar{n}), \quad \eta \in \left(\frac{1}{2}, 1\right], \quad (46)$$

and its second derivative with respect to η can be computed:

$$\frac{d^2 L(\eta, \bar{n})}{d\eta^2} = \bar{n}^2 \left(\frac{1}{(1+(1-\eta)\bar{n})(1-\eta)\bar{n}} - \frac{1}{(1+\eta\bar{n})\eta\bar{n}} \right) \quad (47)$$

$$\geq 0, \quad \eta \in \left(\frac{1}{2}, 1\right]. \quad (48)$$

Hence we conclude that $L(\eta, \bar{n})$ is convex in η on $[0, 1]$ and for every $\bar{n} > 0$. ■

Lemma 3: The multiple-mode lower bound

$$L^M(\boldsymbol{\eta}, \bar{n}) \triangleq \max_{\substack{\bar{n}_i \geq 0, \\ \sum_{i=1}^m \bar{n}_i = \bar{n}}} L(\eta_i, \bar{n}_i) \quad (49)$$

is both convex and Schur-convex in $\boldsymbol{\eta}$.

Proof: First note that $L^M(\boldsymbol{\eta}, \bar{n})$ is symmetric in the elements of $\boldsymbol{\eta}$, hence convexity implies Schur-convexity [7]. To prove convexity, consider any two vectors $\boldsymbol{\eta}^a, \boldsymbol{\eta}^b$ and their mean $\boldsymbol{\eta}^c \triangleq (\boldsymbol{\eta}^a + \boldsymbol{\eta}^b)/2$. Suppose that \bar{n}^* achieves $L^M(\boldsymbol{\eta}^c, \bar{n})$:

$$L^M(\boldsymbol{\eta}^c, \bar{n}) = \sum_{i=1}^m L(\eta_i^c, \bar{n}_i^*). \quad (50)$$

We have

$$\begin{aligned} & (L^M(\boldsymbol{\eta}^a, \bar{n}) + L^M(\boldsymbol{\eta}^b, \bar{n}))/2 \\ & \geq \left(\sum_{i=1}^m L(\eta_i^a, \bar{n}_i^*) + \sum_{i=1}^m L(\eta_i^b, \bar{n}_i^*) \right)/2 \end{aligned} \quad (51)$$

$$\geq \sum_{i=1}^m L(\eta_i^c, \bar{n}_i^*) \quad (52)$$

$$= L^M(\boldsymbol{\eta}^c, \bar{n}). \quad (53)$$

Here: (51) follows by lower-bounding the maxima over \bar{n} with the specific choice $\bar{n} = \bar{n}^*$; and (52) by the convexity of $L(\cdot, \bar{n})$ as in Lemma 2. Hence $L^M(\boldsymbol{\eta}, \bar{n})$ is convex in $\boldsymbol{\eta}$. ■

We are now ready to prove a lower bound on the private capacity of the multiple-mode wiretap bosonic channel under turbulence which can be expressed using $\mathbb{E}[\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}]$.

Theorem 6: Let $\{\mu_1, \dots, \mu_m\}$ denote the diagonal elements of $\mathbb{E}[\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}]$, then

$$C_P^M(\mathbf{T}, \bar{n}) \geq L^M(\boldsymbol{\mu}, \bar{n}), \quad (54)$$

where $L^M(\cdot, \cdot)$ is defined as in (49).

Remarks: As discussed in Section IV-B, the choice of basis for \mathbf{T} does not affect the private capacity of our channel model, so Theorem 6 holds when $\boldsymbol{\mu}$ denotes the diagonal terms of $\mathbb{E}[\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}]$ in any basis. In particular, it holds if $\boldsymbol{\mu}$ denotes the eigenvalues of $\mathbb{E}[\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}]$, and this choice of $\boldsymbol{\mu}$ provides the tightest bound obtainable in this manner. Toward that end, the turbulence calculations from [8] will permit this lower bound to be evaluated for transmitters that use focused-beam, Hermite-Gaussian, or Laguerre-Gaussian spatial modes.

Proof: Let $\{M_1, \dots, M_m\}$ denote the random diagonal elements of the random matrix $\mathbf{T}_{ab}^\dagger \mathbf{T}_{ab}$. We have the following chain of inequalities:

$$C_P^M(\mathbf{T}, \bar{n}) \geq \mathbb{E}[L^M(\mathbf{H}, \bar{n})] \quad (55)$$

$$\geq \mathbb{E}[L^M(\mathbf{M}, \bar{n})] \quad (56)$$

$$\geq L^M(\boldsymbol{\mu}, \bar{n}). \quad (57)$$

Here: (56) follows by the Schur-convexity of $L^M(\cdot, \bar{n})$ and the fact that the eigenvalues $\{H_1, \dots, H_m\}$ majorize the diagonal elements $\{M_1, \dots, M_m\}$; and (57) follows by the (normal) convexity of $L^M(\cdot, \bar{n})$. ■

ACKNOWLEDGEMENTS

This research was supported by the DARPA InPho program under ARO Grant No. W911NF-10-1-0416, and by the NSF IGERT program Interdisciplinary Quantum Information Science and Engineering (iQuISE).

REFERENCES

- [1] S. Guha, Z. Dutton, and J. H. Shapiro, "On quantum limit of optical communications: concatenated codes and joint-detection receivers," in *Proc. IEEE Int. Symp. Inform. Theory*, Saint Petersburg, Russia, July 31–August 5, 2011.
- [2] S. Guha, J. H. Shapiro, and B. I. Erkmen, "Capacity of the bosonic wiretap channel and the entropy photon-number inequality," in *Proc. IEEE Int. Symp. Inform. Theory*, Toronto, Canada, July 6–11, 2008.
- [3] M. M. Wolf, D. Pérez-García, and G. Giedke, "Quantum capacities of bosonic channels," *Phys. Rev. Lett.* **98**, 130501 (2007).
- [4] G. Smith, "The private classical capacity with a symmetric side channel and its application to quantum cryptography," *Phys. Rev. A*, **78**, 022306 (2008).
- [5] D. Slepian, "Analytic solution of two apodization problems," *J. Opt. Soc. Am.* **55**, 1110–1115 (1965).
- [6] J. H. Shapiro, "Normal-mode approach to wave propagation in the turbulent atmosphere," *Appl. Opt.* **13**, 2614–2619 (1974).
- [7] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications*. Academic Press, 1979.
- [8] N. Chandrasekaran and J. H. Shapiro, "Turbulence-induced crosstalk in multiple-spatial-mode optical communication," submitted to *CLEO 2012 Conference*, San Jose, CA, May 8–10, 2012.